UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT CINCINNATI

ALEXANDER BUCK, individually and on behalf of all others similarly situated, Plaintiff, v. THE KROGER CO., Defendant.	Case No. 1:21-cv-00279 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Alexander Buck ("Plaintiff" or "Plaintiff Buck"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class members" as defined below) and by and through his undersigned counsel, files this Class Action Complaint against Defendant The Kroger Co. ("Kroger" or "Defendant") and alleges the following based upon personal knowledge of facts pertaining to himself and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Plaintiff seeks to hold Defendant responsible for the damages it caused him and other Class members in the large and preventable data breach that occurred when unauthorized users accessed Accellion, Inc.'s ("Accellion") servers that contained personal information of current and former employees of Defendant (the "Data Breach" or "Breach"). By its Notice of Data Breach letter, Defendant claims that it learned that the Data Breach occurred on January 23, 2021, though Defendant did not provide notice of the data breach to

affected individuals until at least March 11, 2021. However, the Data Breach actually occurred in December of 2020.

2. Accellion was a third-party vendor used by Defendant for secure file transfers.

3. Kroger was aware and had full knowledge that Accellion's data security on the platform Kroger used was lax. In fact, prior to the breach, Accellion encouraged Kroger to move to a newer and more secure transfer platform.

4. Every year millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, some companies still fail to put adequate security measures in place to protect their customers' and employees' data.

5. Defendant, a nationwide supermarket chain, is among those companies which have failed to meet its obligation to protect the sensitive personal identifying information entrusted to them by current and former employees[1].

6. On March 11, 2021, Defendant distributed a Notice of Data Breach in which it announced that it learned on January 23, 2021 that an unknown third party gained unauthorized access to Accellion's software that stored certain employee data. Personal identifying information ("PII") accessed included names, email addresses and other contact information, birthdates, Social Security numbers, and, for some employees, salary information such as net and gross pay and withholdings.

[1] Unless specified otherwise, "employee" as used herein includes former and current employees of Defendant.

7. As a result of Defendant's negligence and failures further discussed herein, Plaintiff's PII was exposed to unauthorized persons.

8. Despite its role in managing so much sensitive and personal information, Kroger failed to utilize a competent third-party data transfer company when handling and/or transferring Kroger's current or former employees' PII, and Kroger chose to use an outdated and unsecure transfer platform.

9. As a condition of employment, Plaintiff and the Class members were required to disclose their PII to Defendant, entrusting Defendant to keep it safe and protected.

10. Plaintiff and those similarly situated relied upon Kroger to maintain the security and privacy of the PII entrusted to it; when providing their PII, they reasonably expected and understood that Kroger would comply with its obligations to keep the information secure and safe from unauthorized access.

11. Defendant collected its employees' sensitive PII. Defendant had an obligation to secure that PII by implementing reasonable and appropriate data security safeguards, as well as ensuring that its third-party vendors were also implementing reasonable and appropriate data security safeguards.

12. As a result of Defendant's failure to provide reasonable and adequate data security and to ensure that its third-party vendors were doing the same, Plaintiff's and the Class members' PII has been exposed to those who should not have access to it. Plaintiff and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly sensitive PII stolen here.

THE PARTIES

13. Defendant, The Kroger Co., is an Ohio corporation with its principal place of business in Cincinnati, Ohio. Defendant is a national supermarket chain. Defendant has nearly 2,800 stores in thirty-five states and has annual sales of more than 121.1 billion. It is one of the world's largest retailers.[2]

14. Currently, Defendant is a publicly traded company listed on the New York Stock Exchange (symbol KR). It has annual revenues exceeding $100 billion. Defendant has more than 453,000 employees and hundreds of thousands of former employees.

15. Plaintiff Alexander Buck is a resident of Valley Center, Kansas. In March 2021, Plaintiff received notice from Defendant by letter dated March 11, 2021 that it improperly exposed his PII to unauthorized third parties. Plaintiff worked for Defendant from 2015-2016.

16. Plaintiff reasonably believed Defendant would keep his PII secure. Had Defendant disclosed to Plaintiff that it utilized outdated services for its file transfers, such as Accellion, and that his PII would not be kept secure and would be kept easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII.

17. Plaintiff suffered actual injury from having his PII exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of his PII—a form of intangible property that the Plaintiff entrusted to Defendant as a condition of his employment; (b) loss of his privacy; (c) time spent directly attributable to the Data Breach having to protect his PII because his PII was stolen from a service paid for and

[2] *See* https://www.thekrogerco.com/about-kroger/.

chosen by Defendant; and (d) imminent and impending injury arising from the increased risk of additional fraud and additional identity theft.

JURISDICTION AND VENUE

18. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one Class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in Ohio, and has sufficient minimum contacts with Ohio.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant knew Accellion's system was inadequate

21. Kroger entrusted Accellion to hold and possess Kroger's employees' personal data. Accellion is a software company that purports to offer secure file-transfer to its customers. Accellion boasts the security of its "firewall" products that are intended to prevent data breaches: "When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[3]

[3] https://www.accellion.com/company/

22. Accellion offers a file-transfer product called "FTA." This self-described "legacy" product is 20 years old[4] and incapable of preventing modern data security threats.

23. Starting April 30, 2021, Accellion will no longer offer its FTA product.[5]

24. For years, Accellion has urged that its customers (such as Kroger) migrate to its newer, more secure product "Kiteworks," which was launched roughly four years ago, yet even though advised to update its security by its own experts Kroger still failed to maintain adequate security.[6]

25. Kroger used Accellion's outdated legacy FTA to transfer the PII of its current and former employees.

26. Accellion's legacy FTA software relied on CentOS 6 to function.

27. In late 2019, CentOS announced it would no longer support CentOS 6 after November 30, 2020.

28. Upon information and belief, the fact that it was no longer supported by CentOS meant that the FTA software would no longer receive expected vulnerability testing and patching.

29. On December 25, 2020, Accellion suffered a massive data breach which exposed the sensitive PII of millions of individuals—including Kroger's employees.

30. The breach occurred after hackers exploited a vulnerability in Accellion's legacy FTA software through traditional SQL injection methodology.

---

[4] https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/

[5] https://www.accellion.com/sites/default/files/resources/fta-eol.pdf

[6] https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/; https://www.accellion.com/sites/default/files/resources/fta-eol.pdfdiversity requirement.

31. As an employer, Kroger required its employees to provide it their sensitive PII.

32. Kroger is fully aware of how sensitive the PII it stores and maintains is. It is also aware of how much PII it collects, uses, and maintains from each Plaintiff or Class member.

33. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the Class Members' PII, Kroger assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII it collected, stored, and shared with Accellion.

B. Defendant's inadequate data security exposes its employees' sensitive PII

34. On or around January 23, 2021, Defendant allegedly learned that unknown third-party cyber criminals gained access to an Accellion server that was used to store Defendant's employee data.

35. PII accessed included names, email addresses and other contact information, birthdates, Social Security numbers, and, for some employees, salary information such as net and gross pay and withholdings, was among the PII that may have been accessed by the hackers.

36. Plaintiff received a letter from Defendant dated March 11, 2021 entitled "Notice of Data Incident." The letter stated that his PII, detailed below, may have been compromised, and included the following information:

> **What Happened?**
>
> We were recently made aware of a data security incident affecting Accellion, which was used by the Kroger Family of Companies, as

well as many other companies, for secure file transfers. Accellion has confirm that an unauthorized third person gained access to certain Kroger Family of Companies files by exploiting a vulnerability in Accellion's file transfer service.

What Information Was Involved?

Impacted information includes names, email address and other contact information, date of birth, Social Security number, and for some associates or former associates, may have also included certain salary information such as net and gross pay and withholdings.

What Are We Doing?

The safety of your personal information is of utmost importance to us. We have discontinued the use of the Accellion service, reported the incident to federal law enforcement, and began an investigation to understand the scope and impact of the incident.

C. It is well established that data breaches lead to identity theft and other harms

22. Plaintiff and Class members have been damaged by the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use and/or viewing of their PII as a result of the Data Breach.

23. Each year identity theft causes tens of billions of dollars of losses to victims in the United States.[7] With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: opening new financial accounts in the victim's name, taking out loans in the victim's name, obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical

[7] *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited March 8, 2021).

services in the victim's name, and may even give the victim's PII to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[8]

24. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell and trade the information on the cyber black-market for years.

25. This is not just speculative. As the FTC has reported, if hackers get access to PII, they ***will*** use it.[9]

26. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[10] Identity thieves can also use the information stolen from Plaintiff and Class members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

27. If cyber criminals also manage to acquire financial information, credit and debit cards, health insurance information, driver's licenses and passports, there is no limit to the amount of fraud to which Defendant has exposed Plaintiff and Class members.

28. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[11] As the GAO Report states, this type of identity theft

---

[8] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited March 8, 2021).

[9] Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited March 8, 2021).

[10] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited March 8, 2021).

[11] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited March 8, 2021).

is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

29. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[12]

30. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

31. There may be a time lag between when sensitive PII is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

32. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various Internet websites making the information publicly available.

---

[12] *Id.* at 2, 9.
[13] *Id*. at 29 (emphasis added).

33. Furthermore, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[14]

34. Defendant's failure to adequately protect Plaintiff's and Class members' PII has resulted in Plaintiff and Class members having to undertake mitigation tasks which would have otherwise been unnecessary, often times requiring extensive amounts of time, telephone calls and, for many of the credit and fraud protection services, payment of money.

35. Defendant's offer of twenty-four months of identity monitoring and identity protection services to Plaintiff and Class members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[15] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

36. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, substantial and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely

---

[14] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited March 8, 2021).

[15] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited March 8, 2021).

reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

37. Plaintiff and the Class members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their PII used against them by spam callers, texters, and emailers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' PII, for which there is a well-established and quantifiable national and international market;

i. Damage to their credit due to fraudulent use of their PII; and/or

j. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

38. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

39. Defendant itself acknowledged the harm caused by the Data Breach by offering Plaintiff and Class members twenty-four months of identity theft monitoring services and identity protection services. Twenty-four months of identity theft monitoring and identity protection services is woefully inadequate to protect Plaintiff and Class members from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class members for the injuries they have already suffered.

D. Defendant failed to comply with Federal Trade Commission requirements

40. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[17] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored

[16] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 8, 2021).

[17] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 8, 2021).

on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

42. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

43. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[20]

44. By knowingly utilizing a third-party vendor with inadequate data security, Defendant failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. Defendant's data security policies and

---

[18] *Id.*

[19] Federal Trade Commission, *Start With Security*, *supra* note 5.

[20] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited March 8, 2021).

practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff and the Class members suffered damages

45. The ramifications of Defendant's failure to keep current and former employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[21]

46. The PII belonging to Plaintiff and Class members is private, sensitive in nature, and was left inadequately protected by Defendant, who did not obtain Plaintiff's or Class members' consent to disclose such PII to any other person as required by applicable law and industry standards.

47. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

48. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately implement data security measures, despite its obligations to protect current and former employees' PII.

---

[21] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed March 8, 2021).

49. Had Defendant remedied the deficiencies in its data security systems, as well as those of its third-party vendors, and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its third-party vendors' systems and, ultimately, the theft of PII.

50. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have already experienced and are at continuing risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

51. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[22]

52. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII,
b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,
c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to

[22] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed March 8, 2021).

efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

53. In addition to a remedy for the economic harm, Plaintiff and the Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

F. Defendant's delay in identifying and reporting the breach caused additional harm

54. Affected current and former employees were not notified of the Data Breach until March 11, 2021, months after the Data Breach occurred, thus depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

55. As a result of Defendant's negligence and delay in detecting and notifying current and former employees of the Data Breach, the risk of fraud for Plaintiff and Class members has been driven even higher.

56. Kroger's letters to Plaintiff and members of the Class were patently deficient because they failed to disclose the full range of information that may have been compromised in the breach, downplayed the risk its customers and employees face as a result of the breach,

and failed to provide customers and employees with important information such as when the breach occurred, how the breach occurred, or the number of individuals affected.

57. For example, the letter received by customers and/or employees state: "We learned that the Accellion incident impacted Kroger's files on January 23, 2021, took immediate action, and we discontinued use of Accellion's services and investigated the scope and impact of the incident." This falsely leads recipients of the letters to believe that the data breach occurred on January 23, 2021. In reality, the breach occurred in December of 2020.

58. The letter also falsely implies that the decision to discontinue Accellion's services was timely and provided a benefit to the customers and employees affected by the breach, when in fact, Kroger had prior knowledge Accellion's services were deficient yet failed to act, and the decision to discontinue Accellion's services had absolutely no impact on the vast amounts of data exposed.

59. The letter downplayed the harmful effects to customers and employees of the breach by stating, in the second sentence, that Kroger has "no indication of fraud or misuse of your personal information as a result of this incident." The fact that Kroger itself had not detected fraud or misuse at the time the letter was written is meaningless; employees were (and remain) at imminent risk of identity theft and other fraud—it is common sense that such fraud or misuse was the reason criminals obtained the data in the first place.

60. Furthermore, the fact that Kroger had not detected fraud or misuse does not mean that such incidents had not already occurred—indeed, Kroger's letter encouraged Plaintiff and the Class Members to "[b]e vigilant for the next 12 to 24 months" and told them

that if they see suspicious or unusual activity on their accounts, **not to tell Kroger**, but to report it to someone else.

CLASS ACTION ALLEGATIONS

61. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and the following proposed Nationwide Class, defined as follows:

> All persons residing in the United States who are employees or former employees of Kroger or any of its affiliates, parents, or subsidiaries, who had their PII compromised as a result of the Data Breach that occurred in or around December 2020.

62. In addition, Plaintiff brings this action on behalf of himself and the following proposed Kansas subclass defined as follows:

> All persons residing in the State of Kansas who are employees or former employees of Kroger or any of its affiliates, parents, or subsidiaries, who had their PII compromised as a result of the Data Breach that occurred in or around December 2020.

63. Both the proposed National Classes and the proposed Kansas subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

64. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Kroger; anyone employed by counsel in this action; and any judge or magistrate judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

65. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

66. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein,

b. Whether Defendant's inadequate data security measures were a cause of the data security breach,

c. Whether Defendant owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII,

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII,

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the data security breach,

f. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class members' PII in violation of Section 5 of the FTC Act,

g. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

h. Whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

67. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

68. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner.

69. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

70. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to

all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiff and the Class)

71. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

72. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, ensuring that Plaintiff's and Class members' PII in possession of Defendant's third-party vendors was adequately secured and protected.[23]

73. Defendant owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its systems, and those systems of its third-party vendors, adequately protected the PII of its current and former employees.

74. Defendant owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII

[23] Several courts have recognized a common law duty to safeguard data from cyberattacks. *See, e.g.*, *Wines, Vines & Corks, LLC v. First Nat'l of Nebraska, Inc.,* No. 8:14-CV-82, 2014 WL 12665802 (D. Neb. Aug. 20, 2014); *In re Target Corp. Customer Data Sec. Breach Litig.,* 309 F.R.D. 482, 487 (D. Minn. 2015); *Savidge v. Pharm-Save, Inc.,* No. 3:17-CV-00186-TBR, 2017 WL 5986972 (W.D. Ky. Dec. 1, 2017)**;** *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

of its current and former employees, as well as sharing it with third-party vendors with inadequate security systems in place, and the critical importance of adequately securing such information.

75. Plaintiff and members of the Class entrusted Defendant with their PII with the understanding that Defendant would safeguard their information, would not store the information longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

76. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Defendant's misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Data Breach, including failing to ensure its third-party vendors were adequately safeguarding Plaintiff and Class members' PII.

77. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security and disseminating it to its third-party vendors. Defendant knew about – or should have been aware of - numerous, well-publicized data breaches affecting businesses in the United States.

78. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class members, and by failing to ensure its third-party vendors were providing fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class members.

79. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

80. Because Defendant knew that a breach of its systems – or its third-party vendors' systems - would damage thousands of current and former Defendant's employees,

including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

81. Defendant had a special relationship with Plaintiff and Class members by virtue of their being current employees or former employees of Defendant. Plaintiff and Class members reasonably believed that Defendant would take adequate security precautions to protect their PII.

82. In light of this special relationship, Defendant required Plaintiff and Class members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, passport numbers and other personal information.

83. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

84. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness with regard to providing the agreed-upon compensation and other employment benefits to Plaintiff and Class members and protecting Plaintiff's and Class members' PII.

85. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably accessed, Defendant negligently failed to observe and perform its duty.

86. Plaintiff and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe.

87. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' PII.

88. Through Defendant's acts and omissions, including Defendant's failure to

provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members during the time it was within Defendant's possession or control.

89. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third-party hacker to access a server containing current and former employee PII, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect its current and former employees' PII.

90. Plaintiff and the Class members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiff and the Class members is the type of injury Section 5 of the FTC Act was intended to prevent.

91. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiff and Class members have suffered, as Plaintiff has, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic

and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

92. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

93. Defendant offered employment to Plaintiff and Class members, in exchange for compensation and other employment benefits. Defendant required Plaintiff and Class members to provide their PII, including names, addresses, dates of birth, Social Security numbers, bank account information, email addresses, and other personal information.

94. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

95. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class members would provide their PII in exchange for the prospect of employment and benefits provided by Defendant.

96. These agreements were made by Plaintiff or Class members being employed by Defendant.

97. It is clear by these exchanges that the parties intended to enter into an

agreement and mutual assent occurred. Plaintiff and Class members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Defendant presumably would not have taken Plaintiff's and Class members' PII if it did not intend to provide Plaintiff and Class members compensation and other employment benefits.

98. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure and/or use.

99. Plaintiff and Class members accepted Defendant's employment offer and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

100. Plaintiff and Class members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendant.

101. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII.

102. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class members violated the purpose of the agreement between the parties: Plaintiff's and Class members' employment in exchange for compensation and benefits.

103. Defendant was on notice that its third-party vendors' systems could be vulnerable to unauthorized access yet failed to invest in proper safeguarding of Plaintiff's and Class members' PII.

104. Instead of spending adequate financial resources to safeguard Plaintiff's and Class members' PII, which Plaintiff and Class members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its

implied contracts it had with Plaintiff and Class members.

105. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class members, Plaintiff and the Class members suffered injury as described in detail in this Complaint and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Confidence
(On behalf of Plaintiff and the Class)

106. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

107. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII that Plaintiff and Class members provided to Defendant.

108. Plaintiff's and Class members' PII constitutes confidential, novel, and secret information. Indeed, Plaintiff's and Class members' dates of births cannot be changed, and their Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim. Additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

109. Plaintiff and Class members were required to communicate their confidential, novel, and secret PII to Defendant.

110. Defendant, as Plaintiff's and Class members' employer, was in a position of trust and confidence.

111. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

112. Plaintiff and Class members provided their respective PII to Defendant with

the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

113. Defendant voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

114. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

115. As a direct and proximate result caused by Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages.

116. But for the unauthorized disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

117. Defendant's disclosure of Plaintiff's and Class members' PII constituted a violation of Plaintiff's and Class members' understanding that Defendant would safeguard and protect the confidential, novel, and secret PII that Plaintiff and Class members were required to disclose to Defendant, and constituted a use by Defendant to the injury of Plaintiff and Class members.

118. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of the unauthorized disclosure of Plaintiff's and Class members' PII. Defendant knew its third-party vendors' computer systems and technologies used for

accepting and securing Plaintiff's and Class members' PII had numerous security and other vulnerabilities that placed Plaintiff's and Class members' PII in jeopardy.

119. As a direct and proximate result of Defendant's breaches of confidence, and Defendant's negligent usage of Plaintiff's and Class members' PII while the PII was in Defendant's possession, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Class)

120. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

121. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its employees' PII, to act primarily for the benefit of those employees,

including Plaintiff and Class members. This duty included the obligation to safeguard Plaintiff's and Class members' PII and to timely notify them in the event of a data breach.

122. In order to provide Plaintiff and Class members compensation and employment benefits, Defendant required that Plaintiff and Class members provide their PII.

123. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class members' PII for the benefit of Plaintiff and Class members in order to provide Plaintiff and Class members compensation and employment benefits.

124. Defendant further breached its fiduciary duties owed to Plaintiff and Class members as former employees by failing to remove and otherwise destroy Plaintiff's and Class members' PII from Defendant's systems, as Defendant's employment relationship had ceased and Defendant no longer had any valid purpose for the maintenance and storage of that data.

125. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to properly monitor its third-party vendors whose systems contained Plaintiff's and Class members' PII. Defendant further breached its fiduciary duties owed to Plaintiff and Class members by failing to timely notify and/or warn Plaintiff and Class members of the Data Breach.

126. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII;

(e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

127. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses. As such, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Class)

128. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

129. As described above, when Plaintiff and the Class members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect their PII and to timely notify them in the event of a data breach.

130. These exchanges constituted an agreement between the parties: Plaintiff and Class members were required to provide their PII in exchange for employment and benefits provided by Defendant. These agreements were made by Plaintiff or Class members in the

course of their employment by Defendant.

131. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Defendant presumably would not have taken Plaintiff's and Class members' PII if it did not intend to provide Plaintiff and Class members compensation and other employment benefits.

132. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

133. Defendant's failure to implement adequate security measures to protect the PII of Plaintiff and Class members constituted a denial of Plaintiff's and Class members' expected benefit of the contract between the parties.

134. Defendant's lack of diligence with regard to ensuring that its third-party vendors were implementing adequate security measures to protect the PII of Plaintiff and Class members constituted a denial of Plaintiff's and Class members' expected benefit of the contract between the parties and evaded the spirit of the transaction between the parties.

135. Plaintiff and Class members did not receive the benefit of the bargain with Defendant, because their providing their PII was in exchange for Defendant's implied agreement to keep it safe.

136. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

137. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and

regulations when it engaged in unlawful practices under other laws. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class members' PII; storing the PII of former employees despite any valid purpose for the storage thereof ceasing upon terminating the relationship with those individuals; and failing to disclose to Plaintiff and Class members at the time they provided their PII to it that Defendant's data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

138. Plaintiff and Class members did all or substantially all the significant things that the contract required them to do.

139. Likewise, all conditions required for Defendant's performance were met.

140. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class members' rights to receive the full benefit of their contracts.

141. Plaintiff and Class members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

142. Defendant is liable for this breach of these implied covenants whether or not it is found to have breached any specific express contractual term.

143. Plaintiff and Class members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses, in amounts to be determined at trial

SIXTH CAUSE OF ACTION

Violation of the Kansas Consumer Protection Act
Kan. Stat. Ann. §50-623, *et seq*.

(On behalf of Plaintiff and the Kansas Subclass)

144. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

145. Defendant violated the Kansas Consumer Protection Act (Kan. Stat. Ann. §50-623, *et seq*.) by failing to prevent Plaintiff's and Kansas Subclass members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to ensure its third-party vendors were implementing and maintaining reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and Kansas Subclass members.

146. Defendant is a "supplier" pursuant to Kan. Stat. Ann. §50-624(l) that engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions" pertaining to employment services in Kansas, including but not limited to the following:

a. Defendant mispresented material facts by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Kansas Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Defendant misrepresented material facts to Plaintiff and the Kansas Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Kansas Subclass members' PII;

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Kansas Subclass members' PII;

d. Defendant engaged in deceptive, unfair and unlawful trade acts or practices by

failing to maintain the privacy and security of Plaintiff's and Kansas Subclass members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. §45);

e. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff and Kansas Subclass members in a timely and accurate manner, contrary to the duties imposed by Kan. Stat. Ann. §50-7a02(s).

147. Plaintiff and the Kansas Subclass members are considered "consumers" pursuant to the Kansas Consumer Protection Act, and their employment with Defendant constituted a "consumer transaction" in that it consisted of services provided (Kan. Stat. Ann. §50-624(c).

148. Defendant violated the Kansas Consumer Protection Act, Kan. Stat. Ann. §50-623, *et seq*., when it engaged in fraudulent and deceptive conduct that created a likelihood of confusion and misunderstanding by assuring Plaintiff and the Kansas Subclass members that their PII would be kept safe and unobtainable from unauthorized third persons.

149. As a direct and proximate result of Defendant's acts, Plaintiff's and the Kansas Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

150. As a direct and proximate result of Defendant's acts, Plaintiff and the Kansas Subclass members were injured and lost money or property, including but not limited to the loss of Plaintiff's and Kansas Subclass members' legally protected interest in the confidentiality and privacy of their PII, damages, and additional losses as described above.

151. Defendant knew or should have known that its third-party vendors' computer

systems and data security practices were inadequate to safeguard Plaintiff's and the Kansas Subclass members' PII and that the risk of a data breach or theft was high. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the Kansas Subclass members.

152. To their detriment, Plaintiff and Kansas Subclass members relied upon Defendant's acts and its assurances to safeguard their PII.

153. Plaintiff and Kansas Subclass members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe.

154. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. §50-636, including, but not limited to, recovery of actual damages.

155. Plaintiff and the Kansas Subclass members also seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Plaintiff's and the Kansas Subclass members' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Plaintiff's and the Kansas Subclass members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

SEVENTH CAUSE OF ACTION
Negligent Entrustment
(On behalf of Plaintiff and the Class)

156. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

157. Kroger owed a duty to Plaintiff and the Class to adequately safeguard the PII that it required its employees to provide. Part and parcel with this duty was the duty to only

entrust that data to third-party vendors with adequate and reasonable security measures and systems in place to prevent the unauthorized disclosure of such data.

158. Kroger breached this duty by entrusting Accellion with the sensitive PII belonging to its employees when, as described throughout the Complaint, it knew or should have known that Accellion and Accellion's legacy FTA software was incompetent at preventing such unauthorized disclosure.

159. As a direct and proximate result of Kroger's failure to exercise reasonable care in whom it entrusted its employees' sensitive PII, the personal data of Kroger's employees was accessed by ill-intentioned criminals who could and will use the information to commit identity theft or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

160. As a proximate result of this conduct, Plaintiff and Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

EIGHTH CAUSE OF ACTION
Bailment

161. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

162. Plaintiff and the Class delivered their PHI to Kroger for the exclusive purpose of obtaining employment.

163. The PII is intangible personal property belonging to Plaintiff and the Class Members.

164. In delivering their personal data to Kroger, Plaintiff and Class Members intended and understood that Kroger would adequately safeguard their personal data, including by exercising reasonable care in whom it provides its employees' PII.

165. Kroger understood that it had a duty to account for, return, and/or destroy the PII entrusted to it upon request.

166. Kroger accepted possession of Plaintiff's and Class members' PII for the purpose of providing employment to Plaintiff and Class members.

167. A bailment (or deposit) was established for the mutual benefit of the parties.

168. During the bailment (or deposit), Kroger owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal data as well as a duty to safeguard personal information properly and maintain reasonable security procedures and practices to protect such information. Kroger breached this duty when it entrusted its employees' sensitive PII to Accellion through the use of Accellion's outdated legacy FTA software, which Kroger knew or should have known was incapable of providing reasonable security to Kroger's data.

169. Kroger breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII.

170. As a proximate result of this conduct, Plaintiff and the other Class members suffered and will continue to suffer damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated and the Class, respectfully requests the Court order relief and enter judgment in their favor and against Defendant as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein.

B. Plaintiff requests injunctive and other equitable relief as is necessary to protect the interests of the Class, including (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with federal, state and local laws, and best practices under industry standards; (iii) requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected; (iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering it to promptly correct any problems or issues detected by these auditors; (vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii)

requiring Defendant to implement multi-factor authentication requirements; (viii) requiring Defendant to encrypt all PII; (ix) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (x) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner PII no longer necessary for the provision of services; (xi) requiring Defendant to conduct regular computer system scanning and security checks; (xii) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members; and (xiii) requiring Defendant to educate all Class members about the threats they face as a result of the loss of their PII to third parties, as well as steps Class members must take to protect themselves.

C. A judgment awarding Plaintiff and Class members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Defendant pay the costs involved in notifying the Class members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: April 19, 2021

Respectfully submitted,

/s/Brian D. Flick, Esq.
Marc E. Dann (0039425)

Brian D. Flick (0081605)
DannLaw
P.O. Box. 6031040
Cleveland, Ohio 44103
Office: (216) 373-0539
Facsimile: (216) 373-0536
Email: notices@dannlaw.com

William B. Federman, OBA #2853*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

**pro hac vice application forthcoming*

Counsel for Plaintiff and the Putative Class